AD

AD-E403 744

Technical Report ARWSE-TR-15037

STRATEGIES FOR TRANSPORTING DATA BETWEEN CLASSIFIED AND UNCLASSIFIED NETWORKS

Ross D. Arnold

March 2016

U.S. ARMY ARMAMENT RESEARCH, DEVELOPMENT AND ENGINEERING CENTER

Weapons and Software Engineering Center

Picatinny Arsenal, New Jersey

The views, opinions, and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.

The citation in this report of the names of commercial firms or commercially available products or services does not constitute official endorsement by or approval of the U.S. Government.

Destroy this report when no longer needed by any method that will prevent disclosure of its contents or reconstruction of the document. Do not return to the originator.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-01-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (*From - To*)
March 2016	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
STRATEGIES FOR TRANSPORTING DATA BETWEEN CLASSIFIED AND UNCLASSIFIED NETWORKS	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHORS	5d. PROJECT NUMBER
Ross D. Arnold	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army ARDEC, WSEC Fire Control Systems & Technology Directorate (RDAR-WSF-M) Picatinny Arsenal, NJ 07806-5000	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
U.S. Army ARDEC, ESIC Knowledge & Process Management (RDAR-EIK) Picatinny Arsenal, NJ 07806-5000	11. SPONSOR/MONITOR'S REPORT NUMBER(S) Technical Report ARWSE-TR-15037

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Transferring data between unclassified and classified networks is a critical concern of a potential future effort to integrate logistics capability into the tactical applications (TacApps) program. Logistics data is often provided by unclassified networks, while TacApps data will persist on classified networks. In order to mitigate the risk that this obstacle imposes, a literature search was conducted with the goal of identifying methods and technologies available to bridge classified and unclassified networks. Three clearly distinct methods were identified: manual data transfer, the use of a data diode or unidirectional network bridge, and the use of a hardware/software solution called an information security guard. Within these methods, a number of technologies were researched and analyzed for their applicability to TacApps. Only government off-the-shelf and commercial off-the-shelf solutions were examined. Among data diode solutions, the Tactical Army Cross Domain Information Sharing is a good candidate for further research. Among guards, the trusted information system Radiant Mercury appears promising. Further research is required in order to select an appropriate system and quantify additional areas of concern such as bandwidth constraints and available field configurations.

15. SUBJECT TERMS
Mission command Software Battle command Tactical applications (TacApps) BCS3 Command post computing environment Command post client Sustainment Logistics CPC System mission command (S2MC)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Ross D. Arnold
U	U	U	SAR	15	19b. TELEPHONE NUMBER (Include area code) (973) 724-8618

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

CONTENTS

ACKNOWLEDGMENTS

The author would like to thank Timothy Rybarski and Gregory Roehrich for their sponsorship and support, and the Tactical Mission Command Product Management Office for funding the U. S. Army Armament Research, Development and Engineering Center, Picatinny Arsenal, NJ, Weapons and Software Engineering Center to undertake this effort.

INTRODUCTION

In April 2015, the Tactical Applications (TacApps) Team within the U.S. Army Armament Research, Development and Engineering Center, Picatinny Arsenal, NJ, Weapons and Software Engineering Center was assigned a task to analyze the national enterprise data portal (NEDP), a foundational component of the sustainment system mission command. The analysis focused on identifying issues related to potential future efforts to integrate NEDP data feeds into the TacApps architecture. One critical area of concern identified during the analysis was the fact that much of the NEDP data originates from unclassified networks, while the TacApps databases will typically reside on classified networks. Transferring data from unclassified networks to classified and back poses a challenge, especially for large volumes of time-sensitive data. The TacApps chief engineer performed an investigation and literature search into potential technologies and strategies that could mitigate these issues. This report describes the findings of those efforts, including several potential solutions.

STRATEGIES

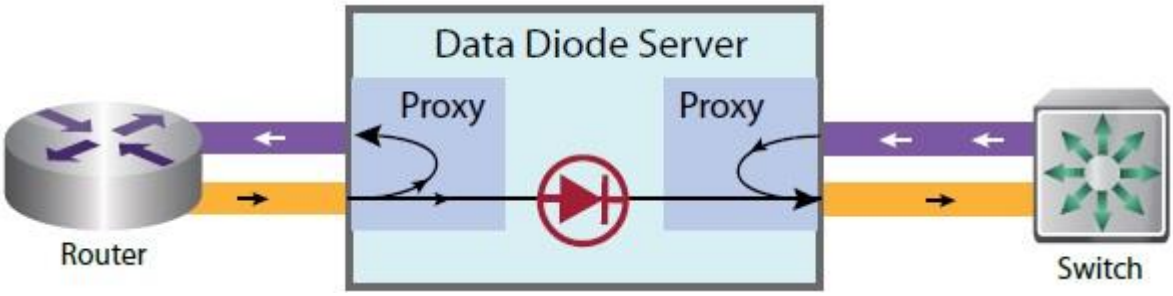
Manual (Swivel-Chair)

The manual method of transferring data between networks, colloquially the “swivel-chair” or “sneaker net” method, involves burning unclassified data to a compact disc, digital video disc, or other form of media. The burned data is then manually loaded onto a machine on the classified network. This method is, not surprisingly, time-consuming and prone to human error (ref. 1). It has been shown to be insecure and lacking in procedural integrity (ref. 1). Despite these drawbacks, it is often the standard method by which data is transferred between networks.

Transferring data from classified to unclassified networks operates in much the same way except that the data must be reviewed by a designated security officer before it can be declassified and moved into the unclassified network. This is even more time-consuming than the reverse, and anecdotal evidence points to the tendency of security officers to naturally err on the side of caution – preventing potentially unclassified data from leaving the classified network in the event of any uncertainty.

Unidirectional Network Bridge (Data Diode)

A unidirectional network bridge, also referred to as a unidirectional security gateway or a data diode, is a combination of hardware and software used to connect two separated networks. The sole purpose of a unidirectional network bridge is to allow data to travel only in one direction; specifically, from one network into another (ref. 1). They are most commonly found in high security environments where they connect two or more networks of differing security classifications. Unidirectional network bridges only physically allow data transfer to occur in one direction, making it physically impossible to transfer data in the opposite direction (refs. 1 and 2). There are several ways to achieve this goal; one popular method is to use a modified fiber optic link as part of the network cable (ref. 1). Using this method, one cable end contains a data transmitter while the other contains a receiver. As a result, it is physically impossible for data to travel in the opposite direction without additional hardware (ref. 1). Often software is employed in some fashion in order to account for the requirements of certain applications such as websites, which require a handshake in order to establish an initial connection before data can be sent (ref. 2). Figure 1 shows a typical data diode hardware/software implementation.



Note: A data diode server terminates full duplex protocols at each end with proxy servers while permitting only one-way traffic between the proxies (ref. 2).

Figure 1
Data diode (ref. 2)

Unidirectional network bridges suffer several major drawbacks. The first of these is the inability to move data from a secure to an insecure network. This results in the use of manual "swivel-chair" or "sneaker net" processes to cover the gap (ref. 1). However, one technical solution to this issue is to use a second unidirectional network bridge to transfer data from a secure to insecure network. This may appear to defeat the purpose of the bridge, but using this solution, both the insertion point and the exit point of data are separate and can be tightly controlled. This does effectively prevent the comingling of data and is used in industry to perform functions such as streaming video and audio from secure to insecure networks (ref. 1).

A second disadvantage lies in the fact that the receiving end of the unidirectional network bridge must have total availability, as any downtime experienced will result in missed data (ref. 1). There is no method to accurately synchronize transferred data. This is of particular concern in environments that require a high level of data integrity. Several methods are available to overcome this problem, such as broadcasting through multiple unidirectional network bridges at once, sending data to multiple receivers, or sending a single file multiple times over the same unidirectional network bridge (ref. 1). None of these methods can guarantee delivery, but they reduce the probability of an error occurring.

A third disadvantage is inherent to the design of the unidirectional network bridge; due to the unidirectional nature of the system, transmission control protocol (TCP) messages cannot be sent over the bridge (ref. 1). The TCP messages require two-way communications; as these are physically prevented by the bridge, TCP is not a viable protocol. Instead, user datagram protocol (UDP) must be used. The UDP is typically used when speed is a higher priority than data integrity, such as in music or video streaming where missed bytes can be ignored by a user. Many defense applications implement their networks using TCP, so if these applications were to require data transfer using a unidirectional network bridge, they would also require code modification.

Finally, all practical implementations of unidirectional network bridges are built by different companies. There are currently no standards body and no specifications system; hence, every implementation is proprietary (ref. 1). This drives up costs and prevents compatibility between different implementations.

Guard

In information security, a guard is a combination of hardware and software used to provide secure data transfer between two information domains (ref. 2). There are many different types of guards with different functionalities, but each guard implements essentially the same basic function: to protect networks at their boundaries and secure data transfer between those networks. In many

respects, a guard is like a firewall, but guards generally provide much more functionality than firewalls in order to address the problems of data exchange between information domains (ref. 2). Guards validate whether or not data transfer can take place by enforcing defined data release policy (ref. 3).

Guards are distinguished from firewalls in three major ways: they have stronger application filtering capability, typically using a reclassifier application to control data transfer between enclaves; they have higher assurance requirements; and they undergo more extensive test and evaluation to provide a higher level of confidence (ref. 4). Several types of guards exist, including multiple single levels of security, multilevel security, low to high, high to low, and bidirectional (ref. 2).

CURRENT TECHNOLOGY SOLUTIONS

Based on the available strategies described previously, a guard is clearly the optimal solution for TacApps from a functional standpoint. Guards allow data to move in both directions provided the constraints are met, and automate the process of reviewing data. In order to provide timely, accurate data to a system requiring frequent updates, a guard may be the only viable solution. However, if moving data from unclassified networks to classified and not necessarily back is acceptable to meet system requirements, a unidirectional network bridge could also be a viable solution as it is likely less costly and easier to maintain. Several of the more promising solutions are described in this report; this is not an exhaustive list.

Data Diode (Government Off-the-shelf): Tactical Army Cross-domain Information Sharing

The Tactical Army Cross Domain Information Sharing (TACDIS) is a small form factor data diode that allows communications from low-level unclassified networks up to high-level secret classified networks. Created at the Communications-Electronics Research, Development and Engineering Center (CERDEC), Aberdeen Proving Ground, MD, the TACDIS tool is an easy-to-connect cable that will enhance situational awareness at higher echelons to protect troops at the tactical edge (ref. 5). It is designed to connect the Rifleman Radio on the low end with Nett Warrior end user devices on the high end. The Nett Warrior program is sponsoring the certification process for the TACDIS. The TACDIS allows the capability to provide unclassified position location information to higher classified systems (ref. 5).

Information from the lower echelons can feed into the higher system at various intervals ranging from every 30 sec to three times per minute (ref. 5). Information regarding bandwidth limits was not available. Fielding for TACDIS is projected to begin in 2015 at the earliest (ref. 5). Figure 2 shows the TACDIS cable.

Figure 2
TACDIS cable (ref. 5)

Data Diode [Commercial Off-the-shelf (COTS)]: Net Optics Tap

Net optics produces a number of both fiber and copper network taps that also serve as unidirectional network bridges. These taps connect network monitoring applications that use unidirectional communications intrinsically, because mirrored copies of network traffic flow one way, to the monitoring tool, and not the other way, from the monitoring tool back to the network (ref. 6). Network taps are therefore natural data diodes, and are a secure way to connect a monitoring tool to the network (ref. 6). Many other tools such as this exist and have been built by other companies. There are likely many viable solutions in this domain.

Guard (Government Off-the-shelf): Radiant Mercury

The trusted information system Radiant Mercury (RM) is a Government off-the-shelf (GOTS) guard solution that successfully provides accredited cross domain solutions to the U.S. Navy, Department of Defense (DoD), and intelligence community (ref. 7). Among other customers, the system is used by the Joint Battle Command Platform Network Operations Center to channel data from unclassified to classified networks. Some of the system's other customers include Combatant Commanders, U.S. Air Force (Shared Early Warning Program), U.S. Army (Blue Force Tracking Program), U.S. Navy (Global Command and Control System-Maritime and Automatic Identification System, Maritime Operations Centers, Distributed Common Ground System-Navy, Tactical Ranges, and numerous other DoD and intelligence agencies (ref. 7).

The RM is a bidirectional guard; it has the capability to channel properly marked data from classified to unclassified networks and back (ref. 7). However, it appears that Intelligence and Security Command has only certified RM to transfer data from unclassified to classified networks. It would likely be difficult to certify a high to low data transfer, but it does appear possible. Also, no information was available regarding bandwidth constraints or other performance parameters. Figure 3 diagrams the RM data flow.

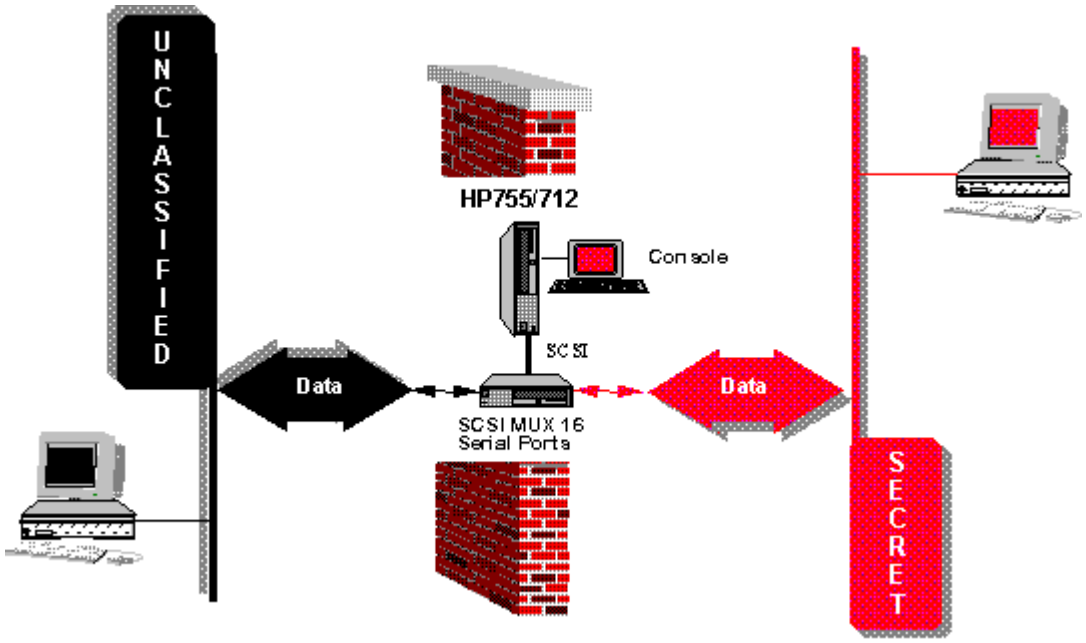


Figure 3
RM data flow

Guard (Government Off-the-shelf): Information Support Server Environment Guard

The information support server environment (ISSE) guard, also called ISSE Star Guard, is a GOTS product developed for the U.S. Air Force. It provides intelligence information, movement of fixed formatted message traffic, extensible markup language, Microsoft office files, emails, text chat, imagery, and many additional types of data across security domains. The system is a bidirectional guard capable of enabling data flow from a single high side network to up to eight low side destinations. At present, there are certified and accredited versions of ISSE fielded at U.S. Government agencies and various other military sites around the world. Information on performance parameters for the ISSE guard was not available.

Guard (Commercial Off-the-shelf): Cross-domain Enterprise All-source User Repository

One commercially available guard solution is the high-speed guard cross-domain security solution used by the cross-domain enterprise all-source user repository (CENTAUR). This guard is COTS software. One drawback of CENTAUR's guard is that it has limited functionality to handle high volume; based on analysis, it can handle pilot deployment, and it can handle zip files at intervals of approximately five minutes or so, depending on the data (ref. 8).

The CENTAUR was prevalent in several key systems during the Empire Challenge 2010 and 2011 exercises at Fort Huachuca, AZ (refs. 3 and 9). During these tests, CENTAUR exchanged intelligence, surveillance, and reconnaissance (ISR) information with the United States and multinational partners at sites worldwide using proven, secure, cross-domain technologies (refs. 3 and 9). The CENTAUR automates the process of pushing data between classified and unclassified systems and enables web-based queries to electronically transfer information (ref. 3). The high-speed guard component validates security, ISR information markings, and data structure prior to transferring the information between security domains (ref. 3).

As of 2011, a CENTAUR system was in use at Fort Gordon, GA, and under test at other domestic and international locations (ref. 3).

CONCLUSIONS

A number of different types of data transfer solutions were examined as a part of this study. Several potential government off-the-shelf and commercial off-the-shelf data diode and guard solutions were identified. This should not be considered an exhaustive list. Additional solutions exist, but this study demonstrates that solutions are available with varying degrees of applicability to the tactical applications (TacApps) effort. If a solution is needed, further down-selection should be performed using a well-established and agreed-upon set of criteria such as cost, specific types of functionality, availability, and others. The solutions described in this report are prime candidates for such a selection.

REFERENCES

1. Slay, J. and Turnbull, B., "The Uses and Limitations of Unidirectional Network Bridges in a Secure Electronic Commerce Environment," paper presented at the INC 2004 Conference, Plymouth, UK, 6-9 July 2004.

2. Maney, C., "Security Issues When Data Traverses Information Domains: Do Guards Effectively Address the Problem?" SANS Institute Reading Room, http://issuu.com/defensestandard/docs/fall2012_book/24, 2004.

3. Raytheon Company, "U.S. Joint Forces Command Deploys Raytheon's CENTAUR System at Empire Challenge First System Awarded Under IDIQ Contract Delivered to U.S. Central Command," Paris, France, 2011. http://investor.raytheon.com/phoenix.zhtml?c=84193&p=irol-newsArticle&ID=1576401

4. Cole, E., Fossen, J., Northcutt, S., Pomeranz, H., SANS Security Essentials with CISSP, "CBK Version 2.1," 2nd ed. Vol. 1. N.p.: SANS Press, 390-391, 2003.

5. Boland, R., Bottom Up! Tool transfers unclassified data to classified networks. "SIGNAL AFCEA International Journal," August 2014.

6. Net Optics, Inc., "Secure, Unidirectional Data Flow with Network Taps," Network Performance Channel GmbH, Langen, Germany, July 2011.

7. United States Navy, "Tactical Command System – MIP," Defense Technical Information Center, PE 0304231N, 2012.

8. Tuttle, R., "Solving A Data Dilemma: Centaur Breaks Down Barriers Hindering Information-Sharing in Coalition Warfare. Defense Standard Quarterly," 24, 26. http://issuu.com/defensestandard/docs/fall2012_book/24, 2012.

9. Raytheon Company, "Raytheon Demonstrates Streaming-Video Transfer Firsts at Empire Challenge 2010," Fort Huachuca, AZ, 2010. http://investor.raytheon.com/phoenix.zhtml?c=84193&p=irol-newsArticle&ID=1467757

DISTRIBUTION LIST

U.S. Army ARDEC
ATTN: RDAR-EIK
RDAR-WSF-M, R. Arnold
Picatinny Arsenal, NJ 07806-5000

Defense Technical Information Center (DTIC)
ATTN: Accessions Division
8725 John J. Kingman Road, Ste. 0944
Fort Belvoir, VA 22060-6218

GIDEP Operations Center
P.O. Box 8000
Corona, CA 91718-8000
gidep@gidep.org

REVIEW AND APPROVAL OF ARDEC TECHNICAL REPORTS

Strategies for Transporting Data Between Classified and Unclassified Networks

Title — Date received by LCSD

Ross D. Arnold

Author/Project Engineer — Report number (to be assigned by LCSD)

X8618 31 — RDAR-WSF-M

Extension Building — Author's/Project Engineers Office (Division, Laboratory, Symbol)

PART 1. **Must be signed before the report can be edited.**

a. The draft copy of this report has been reviewed for technical accuracy and is approved for editing.

b. Use Distribution Statement A__x__, B__, C___, D____, E____, F____ or X____ for the reason checked on the continuation of this form. Reason: ____Operational Use_____

1. If Statement A is selected, the report will be released to the National Technical Information Service (NTIS) for sale to the general public. Only unclassified reports whose distribution is not limited or controlled in any way are released to NTIS.

2. If Statement B, C, D, E, F, or X is selected, the report will be released to the Defense Technical Information Center (DTIC) which will limit distribution according to the conditions indicated in the statement.

c. The distribution list for this report has been reviewed for accuracy and completeness.

Patti Alameda 6/19/15
Division Chief (Date)

PART 2. To be signed either when draft report is submitted or after review of reproduction copy.

This report is approved for publication.

Patti Alameda 6/19/2015
Division Chief (Date)

Andrew Pskowski 6/29/15
RDAR-CIS (Date)